Looking towards the Single European Sky: a Tailored Security Assessment for Future ATM Systems

F. Matarese and P. Montefusco
SESM – Sistemi Evoluti per la Sistemistica e i Modelli S.c.a.r.l., A Finmeccanica Company, Italy

J. Fonseca
University of Coimbra/Polytechnic Institute of Guarda, Portugal

Keywords: *Security, Methodology, Threat, Vulnerability, Risk.*

Abstract

The objective of this paper is the definition of a new methodology for carrying out security risk assessment in the Air Traffic Management (ATM) domain. This process is carried out by modelling the system, identifying the assets, threats and vulnerabilities, prioritizing the threats and proposing countermeasures for the weaknesses found.
ATM security is concerned with securing the ATM assets, to prevent threats and limit their effects on the overall aviation network. This effect limitation could be achieved by removing the vulnerability from the system and/or increasing the tolerance in case of component failures due to attacks.
The security risk assessment methodology proposed is based on what is currently being done by the industry and international organisations (International Civil Aviation Organization (ICAO), Common Criteria (CC), International Standard Organisation (ISO), EUROCONTROL Guidance Material, etc.) and comprises five main stages.
For demonstrative purposes, the methodology is applied to a case study on the Flight Data Processing Subsystem (FDPS), which is a component of many ATM systems.

1 Introduction

ATM security is concerned with securing the ATM assets (including services), to prevent threats and limit their effects on the overall aviation network. This effect limitation could be achieved by removing the vulnerability from the system and/or increasing the tolerance in case of component failures due to attacks.

Recent ATM vulnerabilities discovered and attacks executed (e.g. refer to [1]), prove that the security of these systems is always under the spotlight, which is also confirmed by public entities (e.g. refer to [2]). Furthermore, the increasing complexity of ATM system(s) due to the pervasiveness of emerging technologies and growing number of daily flights create the conditions for the rise of unpredicted threats that may potentially turn into dramatic events. This is also driven by the on-going update of legacy systems with new technologies and their connection to innovative systems, which creates a new environment with new threat vectors, for which these systems were not prepared when they were designed. Thereby, given that the ATM plays a critical role in supporting the overall airspace/aviation system, the security risk assessment of ATM should be a major concern and a top priority.

Presently, the ICAO Security Manual for Safeguarding Civil Application, one of the main references for threat and risk assessment in the ATM domain, offers little help in identifying and prioritising threats according to time and budget constraints. On the other side, new guidelines are on the way, such as those currently being developed in the Sub Work Package (SWP) 16.2 of the Single European Sky ATM Research (SESAR) project, which focus on ATM security framework, methodology, tools and best practices.

As a consequence, the security risk assessment methodology proposed in this paper can be seen as generic, as it is not bound to any technological or implementation constraints, so it can be applied to most ATM systems. In fact it is based on an abstract model defining assets, threats and vulnerabilities related to any ATM system. In fact, it addresses the following objectives:

- To be adopted either by state-of-the-art ATM systems as well as legacy systems allowing the assessment of the new risks that their interconnection may (and will) introduce.
- To be based on existing and well established safety standards already in use by the industry, including the ICAO, the CC, the ISO 270xx, etc. and extend them to cover the ATM security scenario. For example, although widely adopted, the CC does not provide the procedures that should be used to assess the security of the system, whereas the risk assessment methodology that we present addresses this aspect.
- To be complementary with the risk assessment methodology currently being developed within SESAR and other EU projects in ATM security.

2 Security Assessment Methodology

The proposed methodology is based on what is currently being done by the industry and it comprises five main stages that should be revisited during the development and periodically, after the deployment of the ATM system. The methodology is the synthesis of SESAR/ICAO ATM security guidelines and of Microsoft Threat Modelling for the software related threats:

1. **Assets identification**. The ATM system is formally decomposed using Use Cases or Data Flow Diagrams (DFD) to obtain the list of assets and their interconnections. The technique used is complemented with information about trust (or privilege) boundaries between entities.
2. **Threat analysis**. This stage involves determining the possible threats to each asset identified in the previous stage. The following groups of security attributes are used to obtain and classify the threats: the widely accepted set consisting of Confidentiality, Integrity and Availability, or a more detailed view consisting of Authentication, Integrity, Non-repudiation, Confidentiality, Availability and Authorization. It is also in this stage where the Fault Tree model of the threats of each asset is built.
3. **Vulnerability assessment**. Closely related to the threats, vulnerabilities also drive the respective countermeasures, which will be implemented in the last stage, according to the risk analysis outcome.
4. **Risk analysis**. This allows prioritizing the threat mitigation by directing the resources to the most critical threats first. Risk is a measure of the threat impacts to the system vs. the probability of that threat to occur. Several schemes to obtain the likelihood of the occurrence of the threat may be used, some of them based on the outputs that can already be obtained from the SESAR project.
5. **Countermeasure identification/risk treatment**. This provides the mitigation procedures that need to be executed in order to eliminate the threat or limit its effect to an acceptable residual level. They are closely related to the specific threat they apply to and to the target vulnerabilities. The set of countermeasures/security controls are the most important output from this security

assessment methodology as they can be seen as the recommendations or the security requirements for the ATM under assessment.

2.1 Assets identification

An asset is something of value to the Organisation. In general, technological assets combine logical and physical assets and can be grouped into the following categories:

- **Information.** Documented (paper or electronic) data or intellectual property used to meet the mission of an Organisation.
- **Software.** Software applications and services (such as operating systems, database applications, networking software, office applications, custom applications, etc.) that process, store, or transmit information.
- **Hardware.** Physical devices needed for the proper functioning of the Organisation (such as workstations, servers, etc.). This asset normally focus solely on the replacement costs for physical devices.
- **People.** The people in an Organisation that possess unique skills, knowledge, and experience and that are difficult to replace.

2.2 Threat analysis

An ATM system consists of a set of hardware, software and communication assets, operated by several users with different operation statuses. Threat assessment and risk management together form the basis of a viable and cost effective security response to threats that could target ATM system. One of the most difficult tasks for security professionals is devising an effective security plan that correlates to the threat. Accurately identifying the threat or threats must be the first step in the process. Our challenge is to perform a quantitative analytical approach will be used to perform threat assessment.

In devising a threat assessment methodology, it is preferable to use a systematic and quantifiable approach. Therefore, the threat assessment proposed to evaluate the threats affecting the ATM system uses a quantitative analytical approach. The structure of this methodology employs three core principles of security: *identify*, *implement* and *sustain*.

In undertaking the task of assessing the threats, there are several sources of empirical evidence and statistical data available in the fields of intelligence and security from which to form an analysis of past trends of acts of unlawful interference. In order to provide decision-makers with a current and credible threat assessment, however, multiple sources of information should be explored. Threat and vulnerability criteria have to be determined before conducting the assessment by deciding on *focal points/hot spots*. Focal points can be defined as those factors or criteria that are estimated to have the most weight or value in a given process.

This methodology utilises two facets of analysis that together form a credible means of assessing the threat and determining a security response through application of risk management measures.

First, it must be understood that a *deliberate* act of unlawful interference must, by definition, be premeditated and carried out with *purpose* by the perpetrators. This means that someone has a reason to conduct an unlawful act and thus proceeds to plan and execute the act. Therefore, before assessing how an act of unlawful interference may be carried out against a target, the analyst should first consider the reasons why an unlawful act would be committed and the probability of its being committed.

The next step would be to create a working tool to assist in the assessment process: the *Vulnerability Matrix*. The Vulnerability Matrix forms the final analysis for a follow-on risk management process. It covers security threat categories, which can be adapted to assess the threat directed at a potential target or to evaluate the security posture of a part of the system.

Security professionals have long recognized that implementing increased preventive measures commensurate with a higher level of

threat has an associated expense that may become a heavy financial burden on the resources of an Organisation. It is therefore considered more effective to deploy defences where and when they are most needed rather than applying them universally. This concept is called risk management.

Standards consist of a minimum set of security control measures that are expected to be applied equally at international level regardless of the threat environment impacting on operations. While these arrangements were established to ensure minimum uniform standards, no specific standards exist to address variable threat conditions. Whenever an Organisation introduces additional security measures to meet a higher threat level, it may find that implementation is difficult to sustain, especially when the extra measures have not been tailored to the specific threat. Therefore, once an Organisation has properly assessed the nature and level of threat within its own territory, it can then apply appropriate enhanced measures. Organisations can profit of a risk management approach whereby enhanced measures are implemented either to prevent an unlawful act from being committed or, at a minimum, to mitigate any consequences resulting from an unlawful act.

2.3 Vulnerability assessment

A vulnerability assessment is a systematic, point-in-time examination of an Organisation's technology base, policies, and procedures. It includes a complete analysis of the security of an internal environment and its vulnerability to internal and external attacks.

Technology-driven assessments generally:

- Use standards for specific IT security activities (such as hardening specific types of platforms).
- Assess the entire computing infrastructure.
- Use (sometimes proprietary) software tools to analyze the infrastructure and all of its components.
- Provide a detailed analysis showing the detected technological vulnerabilities and possibly recommending specific steps to address those vulnerabilities.

2.4 Risk analysis

According to the ISO GUIDE 73:2002, "Risk is the combination of the probability of an event and its consequences". Inversely, an enterprise manager should decide to make a financial effort to harden a specific asset if the cost of securing it is less than the risk of loss of the asset. In other words, the manager must be sure that the cost of security in every transaction involving the asset is less than the risk of loss. This is the foundation of security risk management, as detailed by Dan Geer [5].

In fact security can be seen as risk management, because we do not want to spend too much on security, comparing to what assets we are protecting. Many times, the big questions posed in an enterprise when it needs to calculate the budget is the measure of the potential loss and lack of knowledge of where it is likely to occur.

A Threat is, in a general approach, anything that might trigger a Risk. However, it is important to point out that a Threat is not directly connected to Risks. A Threat is effective only if it is connected to a Vulnerability. The Risk is thus dependant on the Vulnerability rather than on the Threat itself. If there is a Vulnerability but there is no Threat using it, the Risk remains. Hence, Threats are mitigated through Vulnerability Analysis over the Assets. According to the Vulnerability Analysis, the Threats can be eliminated or reduced to a point where the value of the Risk is acceptable. The process of mitigating the Vulnerabilities is on the scope of the Security Policies and it is implemented with the Countermeasures. The Security Framework will define the Security Policy and the Risk Management Process to secure ATM system.

At the system level, the risk deliberated can be defined by the following formula:

$$Risk = Likelihood\ of\ the\ Threat * Vulnerability * Consequences\ of\ the\ Exploitation \quad (1)$$

The assessment of likelihood takes into account statistical analyses. The assessments of the consequences in terms of loss of security will be considered as the consequence on the operational reliability in the sense that each threat scenario will be evaluated regarding the consequence of the loss of a corresponding security criteria and cost of the primary asset on the operational reliability.

2.5 Countermeasure identification/risk treatment

The main purpose of any security countermeasure is prevention. Therefore, after the first step to *identify* the threat or threats is completed, the next task is to devise an appropriate security response commensurate with that threat. This task employs the *implement* principle.

If the assumption is made that potential perpetrators with the intention to interfere can defeat a security system if given enough information, time and opportunity, then the logical objective is how best to deter the perpetrators from carrying out a successful act of unlawful interference. It is therefore essential that the implementation of suitable preventive security measures be considered.

This operational intervention leads to the third principle, *sustain*, which can be described as an Organisation having the political will and accompanying capability to maintain appropriate reliable security practices. Without the commitment to *sustain* effective security measures, the efficacy of the other principles is diminished.

Countermeasures/security controls will be identified for risk management. A countermeasure is any system, *passive* or *active*, aimed at resolving a risk occurrence. By nature it is reactive rather than proactive, and is aimed at mitigating the loss due to the risk occurrence. Depending on the nature of the risk and the kind of countermeasure, the risk outcome can be only partially mitigated or totally mitigated.

The security countermeasures identified will be spread over the ATM system architecture [4].

3 Case Study: FDPS

For demonstrative purposes, we will apply our methodology to a case study on FDPS, which is a component of many ATM systems. FDPS is based on a open architecture that manages the flight plan data accepting, processing, updating and distributing the trajectories and related data, according to the aircraft current position. It supports the air traffic controllers during the planning and progress phases of the flight. The safety solution implemented by FDPS is based on redundancy, duplicating FDPS instances and managing this distributed system. However, this increases the attack surface of FDPS and creates new entry points that may not be so well protected, like those related with the management and synchronization between FDPS instances. By increasing the safety of FDPS the current design may also be affecting its security and this is where our security assessment methodology can be applied, contributing to uncover and mitigate these issues.

FDPS provides the processing of flight plan data and other related information to support air traffic controllers during the planning and progress phases of flights.

FDPS is based on an open architecture which provides the processing of flight plan data and other related information to support air traffic controllers during the planning and progress phases of flights [3].

FDPS is capable of accepting, processing, updating, distributing and displaying flight data and other information, according with ICAO requirements and in compliance with European Air Traffic Management Programme (EATMP) requirements.

3.1 Assets identification

FDPS is formally decomposed using Data Flow Diagrams to obtain the list of assets and their interconnections.

Flight plans data can be received via the Aeronautical Fixed Telecommunication Network (AFTN) lines, by means of Air Traffic Services (ATS) messages from eligible sources (e.g. the Integrated Initial Flight Plan Processing

System (IFPS)), via the connections with adjacent ATS units, or by means of notification and coordination messages according to EUROCONTROL Standard for On-Line Data Interchange (OLDI).

Furthermore, authorised operators can enter the flight plans.

Whenever an updating of one or more System Flight Plan (SFPL) Data is performed, FDPS provides the updated data to Control Working Position (CWP) operators by means of SFPL and other external users, such as ATS units and Airport Report Office (ARO), by OLDI and ATS messages.

FDPS receives the Monitoring Aids data from the Safety Nets, and it receives Air Traffic Flow Management (ATFM) and ATS messages from Central Flow Management Unit (CFMU), whilst Meteo messages are received from the Meteo/Aeronautical Information Service (AIS) units.

Warning and SFPL data are provided to the Flight Data Assistant.

Furthermore, FDPS sends the diagnostic towards the Control Management System (CMS), and Special Service Request (SSR) Codes data, Configuration and Sectorisation data are sent to FDP Technical Supervisor.

The FDP system is provided in a redundant highly reliable configuration consisting of two identical instances and of distributed logics. It is provided in a redundant configuration to ensure the radar data processing continuity in the system.

FDPS function is required to receive data from and/or send data to a number of other functions and systems. The following table reports FDPS interfaces:

System	Data IN	Data OUT
METEO/AIS Units	MET/AIS messages.	-
CFMU/IFPS	ATS messages.	-
CFMU/TACT	ATFM messages.	FSA message
Aircraft Operators/ARO	ATS Messages; Free Text Messages.	ATS Messages; Free Text Messages.
Adjacent ATS Units	Notification and Coordination messages according to Eurocontrol Standard for	Notification and Coordination messages according to Eurocontrol Standard for
	OLDI; ATS messages; Free Text Messages.	OLDI; ATS Messages; Free Text Messages.
SNET	Monitoring Aids data.	SFPL Data including CFL and trajectory.
ODS	SFPL data update; EXE and PLN orders; Co-ordination data update.	SFPL data; Co-ordination data; Environment data; Warnings.
Flight Data Assistant	SFPL data; RPL data.	SFPL data; Warnings.
FDP Technical Supervisor	Sectorisation data; Configuration data; SSR Codes data.	Sectorisation data; Configuration data; SSR Codes data.
CMS	Configuration orders.	Diagnostics.

Table 1 Data Flow in/out for FDPS

3.2 Threat analysis

FDPS *Hardware security threats* will be investigated. First of all, hardware assets will be categorised, then the following main sources of threats will be analysed:

- *"Physical attack"*

An attack aimed at interrupting, disturbing or in any case damaging the infrastructure. The basic key point is that the attack is done in the physical domain rather than in the information domain.

- *"Environmental threats"*

It can be classified as a special case of Physical attacks, whereas the point is that the threat can also arise from natural causes. Typically, this is the case for climatic phenomenon seismic phenomenon, meteorological phenomenon or flood, which can directly lead to physical damages like fire, water, pollution, major accident, destruction of equipment of media, dust, corrosion, freezing. As a secondary consequence, events like loss of power, failure of telecommunication equipment, electromagnetic or thermal radiation may occur that can bring down electronic and computing systems.

ATM *Software security threats* will be investigated. First of all, software functionalities will be categorised, then the following main sources of threats will be analysed:

- *"Intrusion"*

Any form of attack that leads the attacker to gain unauthorized access to one of the ATM subsystems. The attack can be performed in a number of ways, mainly dependant on software and protocols bugs and vulnerabilities.

ATM *Information security threats* will be investigated. First of all, communication assets and functionalities will be categorised, then the following main sources of threats will be analysed:

- *"Data corruption and stealing"*

It can arise from two different events:

a) Communication security failure
b) System security failure

The first is a consequence of an attack aimed at the communication infrastructure, hence on the data being transmitted. The second kind arises from an attack to a working server or client, i.e., an intrusion.

- *"Identity usurpation"*

It is usually the consequence of a successful attack either at communication or system level, i.e., data stealing or system intrusion. The usurper can use the stolen identity to perform actions of systems that, at first, might seems perfectly legit.

3.3 Vulnerability assessment

The following Computer Software Configuration Items (CSCIs) are included within the software architecture of FDPS:

CSCI	Description
FTF	Fault Tolerance Function: provides services that can be used to handle automatic fail over of applications and data files associated even in the event of operating system, services or hardware failures; when the active node fails, its resources are transferred to the standby node.
XSD	Advanced System Message Dispatcher: provides dispatching of commands and diagnostic messages. XSD produces Node Status Messages using information collected from those CSCIs running inside the same node: • SPV sends information about system peripherals and devices status; • other CSCIs send their internal logical status. XSD collects these data and then sends the node status message periodically to the other system nodes.
SPV	Supervisor: supports for node and process start-up/shutdown, provides the information about the peripherals status and the Node Role (Master/Stand-by) and manages the operator system console in order to view diagnostic messages and to issue commands.
CDB	Common Data Base: handles the whole system configuration, manages the dynamic role of the CWPs and constantly aligns a so called Common Data Base (CDB). CDB is also a Data Base Fault Tolerant and this capability is achieved by its replication on the all system nodes. Consistency of the databases is achieved through a Best Node.
AFS	Advanced FDP Server: responsible for the processing of the core functions of FDPS, including the environment data handling, the flight data processing and distribution, the message handling and data exchange with the other subsystems.
AFJ	Advanced Flight Data Processing Java M.M.I.: provides eligible operators with an HMI supporting the following functionality: • Environment data management, where these information are separated in dynamic data, geographical data and configuration of OLDI and ATS units. • SFPL data management. • Message handling including: generation of one message(OLDI and ATS format), management of wrong and rejected message. • RPL management. • System administration (e.g. line configuration) • Archived data/messages inspection • SSR Code configuration
IOL	Input/Output LAN: provides a set of basic point-to-point and multipoint communication services allowing the exchange of messages among CSCIs of different nodes.
IKS	Internal Kernel SPV: provides communication services allowing the exchange of messages from CSCIs toward LAN. The high level protocol used to communicate over the LAN connecting the computers is the User Datagram Protocol (UDP).

Table 2 FDPS' CSCIs

Only the following CSCIs represent a vulnerability for FDPS: AFS, CDB and IKS, considering the criticality and the impact on the system if affected by malicious attacks.

3.4 Risk analysis

There is no statistic data available related to FDPS attacks to justify a likelihood analysis. For this reason, risk will be evaluated considering just the impact of potential threats on the system and assuming the probability equal to 1 (i.e. 100%). Countermeasures are so identified, initially, on the basis of the threat analysis and the architecture of the system.

The following table reports FDPS risk analysis:

CSCI	Threat	Local Effect	System Effect	Severity
AFS	Data corruption and stealing: loss of message coming from external networks (ATS, meteo, OLDI messages)	Inability of communicating with external networks. (ATS, meteo, OLDI messages). ATC controller is aware of this. Increased workload.	Loss of message flight data exchanged with external networks	Significant
AFS	Data corruption and stealing: loss of data coming from IOL CSCI	Loss of tracks data. Inability of updating trajectories. ATC controller is not aware of this and continues working with existing flight data.	Corruption of flight data exchanged with CWP	Major
AFS	Data corruption and stealing: undetected corruption of data coming from CDB CSCI	The corrupted message is not recognised. Incorrect activation of flight plan data; incorrect entry of new flight plan data; incorrect cancellation of flight plan data.	Corruption of flight data exchanged with CWP	Major
AFS	Data corruption and stealing: corruption of message toward external networks (ATS, meteo, OLDI messages)	Corrupted messages are checked and discarded by receivers. Inability of communicating with external networks. (ATS, meteo, OLDI messages). ATC controller is aware of this. Increased workload.	Loss of message flight data exchanged with external networks	Significant
AFS	Intrusion: overload of messages that causes a memory leak	Flight data not available at CWP. Loss of automatic advance warning of active flights. Inability of activation of flight plan data; inability of entry of new flight plan data; inability of cancellation of flight plan data.	Loss of flight data exchanged with CWP	Major
AFS	Intrusion: corruption of static data in internal AFS CSCI database	Corruption of static data contained in AFS CSCI database. Incorrect distribution of static data for display. Incorrect flight data references may result in inappropriate actions being taken by the CWP operator.	Corruption of flight data exchanged with CWP	Major
AFS	Identity usurpation: loss of connection with internal AFS CSCI database or algorithm failure	Flight data not available at CWP. Loss of automatic advance warning of active flights. Inability of activation of flight plan data; inability	Loss of flight data exchanged with CWP	Major

CSCI	Threat	Local Effect	System Effect	Severity
		of entry of new flight plan data; inability of cancellation of flight plan data.		
CDB	Data corruption and stealing: loss of received message from AFS CSCI	The common database is not updated.	No effect	Significant
CDB	Data corruption and stealing: detected corruption of received message from AFS CSCI	The corrupted message is discarded and the common database is not updated.	No effect	Significant
CDB	Data corruption and stealing: undetected corruption of received message from AFS CSCI	The corrupted message is not recognised and the common database is contaminated.	Corruption of flight data exchanged with CWP	Major
CDB	Data corruption and stealing: loss of sent message toward AFS CSCI	AFS doesn't receive data from CDB but is aware of it. Inability to activate flight plan data, to enter new flight plan data and to cancel flight plan data.	Loss of flight data exchanged with CWP	Major
CDB	Data corruption and stealing: loss of sent message toward CWP	ATC controller doesn't receive updated data from FDP system but is aware of it. Flight data not available at CWP. Loss of automatic advance warning of active flights.	Loss of flight data exchanged with CWP	Major incident
CDB	Data corruption and stealing: undetected corruption of sent message toward CWP	The corrupted message is not recognised. Incorrect distribution of data for display. ATC controller is not aware of this. Incorrect flight data may result in inappropriate actions being taken by the CWP operator.	Corruption of flight data exchanged with CWP	Major
CDB	Data corruption and stealing: undetected corruption of sent message toward AFS CSCI	The corrupted message is not recognised. Incorrect activation of flight plan data; incorrect entry of new flight plan data; incorrect cancellation of flight plan data.	Corruption of flight data exchanged with CWP Loss of message flight data exchanged with external networks	Major
CDB	Intrusion: overload of messages that causes a memory leak	Flight data not available at CWP. Loss of automatic advance warning of active flights. Inability of activation of flight plan data; inability of entry of new flight plan data; inability of cancellation of flight plan data.	Loss of flight data exchanged with CWP	Major
IKS	Data corruption and stealing: generic internal failure, inability to manage hardware resources	Flight data not available at CWP. Loss of automatic advance warning of active flights. Inability of activation of flight plan	Loss of flight data exchanged with CWP	Major

CSCI	Threat	Local Effect	System Effect	Severity
		data; inability of entry of new flight plan data; inability of cancellation of flight plan data. An alert is sent to CSCI of FDPS. Messages generated are lost.		

Table 3 FDPS risk analysis

3.5 Countermeasures identification/risk treatment

The set of countermeasures are the most important output from this security assessment methodology as they can be seen as the recommendations or the security requirements for FDPS.

According to the risk analysis, the following countermeasures can be identified in order to limit the effects of attacks that cause corruption of data:

- Syntactic and semantic check algorithms of AFS and CDB CSCIs.
- Syntactic and semantic check algorithms of CWP.

Regarding the loss of data, no countermeasure can be identified internal to FDPS. Other measures can be identified to protect ATM system from intrusions, as encryption and decryption algorithms passwords.

4 Conclusion

The objective of this paper is the definition of a new methodology for carrying out security risk assessment in the ATM domain. This process is carried out by modelling the system, identifying the assets, threats and vulnerabilities, prioritizing the threats and proposing countermeasures for the weaknesses found.

For demonstrative purposes, we have applied our methodology to a case study on FDPS, which is a component of many ATM systems.

The results are:

- the identification of assets, as services given by the system,
- the analysis of threats, as potential attacks,
- the assessment of vulnerabilities, as CSCI of the system are vulnerable because remotely accessible,
- the analysis of risks, considering the effects of successful attacks,
- and, finally, the identification of countermeasures to limit those effects.

The proposed methodology allows the identification of countermeasures in a systematic way. Countermeasures can be adopted as security system requirements at design level. Nevertheless, not all the countermeasures to protect data can be applied, and identified, at subsystem level, so the security assessment has to be performed also at a higher (system) level.

References

[1] Federal Aviation Administration, *Review of Web applications security and intrusion detection in Air Traffic Control Systems*, U.S. Department of Transportation, 2009.

[2] SESAR Definition Phase Project, *D1 Air Transport framework – The current situation*, v3, SESAR Consortium, 2006.

[3] International Civil Aviation Organization, *Procedures for Air Navigation Services - Rules of the Air and Air Traffic Services*, ICAO, Thirteenth Edition, 1996.

[4] International Civil Aviation Organization, *Security Manual for Safeguarding Civil Aviation Against Acts of Unlawful Interference*, ICAO, Sixth Edition, 2002.

[5] Geer, D., *Risk management is still where the money is*, Computer, *36*(12), 129-131, doi:10.1109/MC.2003.1250894, 2003.

Acknowledgments

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013), in the frame of Marie Curie Industry-Academia Partnerships and Pathways Call (FP7-PEOPLE-2008-IAPP), under Grant Agreement No. 230672 ("CRITICAL-STEP" Project).